AMENDMENTS TO THE SPECIFICATION

Please amend the specification as follows:

Please rewrite the paragraph starting on line 22 of page 8 to read:

Certain of the implementations of partial dual encryption described herein utilize an additional (secondary) PID for each duplicated component. These secondary PIDs are used to tag packets that carry duplicated content with an additional encryption method. The PSI is enhanced to convey information about the existence _of_ these new PIDs in such a way that inserted PIDs are ignored by legacy STBs but can be easily extracted by new STBs.

Please rewrite the paragraph starting on line 5 of page 10 to read:

The various embodiments of the invention allow each participating CA system to be operated independently. Each is orthogonal to the other. Key sharing in the headend is not required since each system encrypts its own _packets_ ~~patents~~. Different key epochs may be used by each CA system. For example, packets encrypted with Motorola's proprietary encryption can use fast changing encryption keys using the embedded security ASIC, while packets encrypted with NDS' smart card based system use slightly slower changing keys. This embodiment works equally well for Scientific Atlanta and Motorola legacy encryption.

Please rewrite the paragraph starting on line 18 of page 11 to read:

Both legacy and new set-top boxes can function in a normal manner receiving video in the clear and decrypting the audio in the same manner used for fully decrypting encrypted A/V content. If the user has not subscribed to the programming encrypted according to the above scheme, at best the user can only view the video without an ability to hear the audio. For enhanced security over the video, it _is_ possible to employ other embodiments of the invention (as will be described later) here as well. (For example, the SI may be scrambled to make it more difficult for a non-authorized set-top box to tune to

the video portion of the program.) Unauthorized set-top boxes that have not been modified by a hacker, will blank the video as a result of receipt of the encrypted audio.

Please rewrite the paragraph starting on line 8 of page 12 to read:

In one embodiment of the present invention, the encrypted audio is transmitted as digitized packets over the A/V channel. Two (or more) audio streams are transmitted encrypted according to the two (or more) encryption systems in use by the system's set-top boxes. In order for the two (or more) STBs to properly decrypt and decode their respective audio streams, SI (system information) data are transmitted from the cable system's headend 122 that identifies the particular channel where the audio can be found using a transmitted Service Identifier to locate the audio. This is accomplished by assigning the audio for system A ~~is~~ a first packet identifier (PID) and assigning the audio for system B a second packet identifier (PID). By way of example, and not limitation, the following program specific information (PSI) can be sent to identify the location of the audio for two systems, one using NDS conditional access and one using Motorola conditional access. Those skilled in the art will understand how to adapt this information to the other embodiments of partial encryption described later herein.

Please rewrite the paragraph starting on line 18 of page 16 to read:

In an alternative embodiment, only the video may be dual or multiple encrypted with separate PIDs assigned to each set of encrypted video. While this may provide a more secure encryption for general programming (since video may be more important than audio), the amount of bandwidth savings compared with full dual carriage is only approximately ten percent, since only the audio is shared amongst all the set-top boxes. However, this approach might be used for certain content, e.g. adult and sports, and help reduce the bandwidth overhead for that content while the audio encryption approach may be used for other content types. In the Digital Satellite Service (DSS) transport standard used for the DirecTV™ service, the audio ~~ardio~~ packets can be identified for encryption by use of the service channel identifier (SCID) which is considered equivalent.

Please rewrite the paragraph starting on line 2 of page 17 to read:

Another embodiment consistent with the present invention is referred to herein as time slicing and is illustrated in **FIGURE 3** as system 200. In this embodiment, a portion of each program is encrypted on a time dependent basis in a manner that disrupts viewing of the program unless the user has paid for the programming. This embodiment of the invention can be implemented as partially encrypted video and clear audio, clear video and partially encrypted audio or partially encrypted video and audio. The duration of the time slice that is encrypted, taken as a percentage of the total time, can be selected to meet any suitable desired balance of bandwidth usage~~,~~ and security against hackers. In general, under any of the embodiments described herein, less than 100 percent of the content is encrypted to produce a desired partial encryption. ~~—~~ The following example details partially encrypted video and audio.

Please rewrite the paragraph starting on line 23 of page 17 to read:

With reference to **TABLE 1** below, an exemplary embodiment of a time slice dual encryption scheme consistent with an embodiment of the invention is illustrated. For program 1 having primary video PID 101 and primary audio PID 201, during the first time period, packets having PID 101 and PID201 are encrypted using encryption system A, while the others representing the other programs are sent in the clear. In this embodiment, secondary PIDs are also assigned to both the video and the audio. The secondary PIDs are PID 111 for video and PID 211 for audio respectively for program 1. The packets with the secondary PIDs are encrypted using encryption system B during the first time period. The next eight time periods are sent in the clear. Then for time period 10, packets having any of the above four PIDs are again encrypted followed by the next eight time periods being sent in the clear. In a similar manner, during the second period of program 2 having primary video PID 102 and primary audio PID ~~201~~ 202 are encrypted using encryption system A and packets with their associated secondary PIDs are encrypted using encryption system B, and during the next eight time periods are sent in the clear, and so on. This pattern can be seen clearly in **TABLE 1** by examination of the

first nine rows. Both audio and video packets, or audio alone or video alone can be encrypted according to this technique, without departing from the invention. Also, the audio and video can have their own individual encryption sequence. In **TABLE 1**, P1 indicates time period number 1, P2 indicated time period number 2 and so on. EA indicates that the information is encrypted using CA system A and EB indicates that the information is encrypted using CA encryption system B.

Please rewrite the paragraph starting on line 32 of page 19 to read:

With reference to **FIGURE 3**, system 200 generally depicts the functionality of the cable system headend 222 wherein N channels of clear video ~~204~~ 208 at the headend 222 are provided to an intelligent switch 216 (operating under control of a programmed processor) which routes packets that are to be transmitted in the clear to be assigned a primary PID at 220. Packets that are to be encrypted are routed to both conditional access system A encrypter 218 and to conditional access system B encrypter 224. Once encrypted, these encrypted packets from 218 and 224 are assigned primary or secondary PIDs respectively at 220. System information from 228 and PSI from 229 are ~~is~~ multiplexed or combined with the clear packets, the system A encrypted packets and the system B encrypted packets and broadcast over the cable system 32.

Please rewrite the paragraph starting on line 14 of page 20 to read:

The PSI for a partially scrambled stream is handled slightly differently from the dual audio encryption example above. Essentially, the same SI and PAT PSI information can be sent to both legacy and non-legacy set-top boxes. The difference lies with the PMT PSI information. The legacy set-top box parses the PMT PSI and obtains the primary video and audio PIDs as before. The non-legacy set-top box obtains the primary PIDs like the legacy set-top box but must look at the CA descriptors in the PMT PSI to see if the stream is partially scrambled. The secondary PID is scrambled specifically for a particular CA provider, consequently it makes sense to use the CA descriptor specific to a particular CA provider to signal that PID. The invention can allow more than two CA providers to co-exist

by allowing more than one secondary PID. The secondary PID shall be unique to a particular CA provider. The set-top box ~~know~~ knows the CA ID for the CA it has, and can check all CA descriptors for the relevant one for it.

Please rewrite the paragraph starting on line 24 of page 22 to read:

FIGURE 5 illustrates a process used in the STB 236 having the newly introduced CA system B for decrypting and decoding the received data stream containing C, EA and EB packets having primary and secondary PIDs as described. When a packet is received at 272, it is inspected to see if it has ~~a~~ the primary PID of interest. If not, the packet is examined to see if it has the secondary PID of interest at 274. If the packet has neither the primary or secondary PID, it is ignored or dropped at 278. Any intervening packets between the EA and EB packets that are not the primary or secondary PID are discarded. It is an implementation and mainly a buffering issue whether a decoder can receive multiple EA or EB in a row before receiving the replacement matched EA or EB packet. Also, it is just as easy to detect for secondary packets that come before and not after the primary packet. It is also possible to design a circuit where either case can happen – the secondary packet can be either before or after the primary packet. If the packet has the primary PID of interest, the packet is examined at 284 to determine if it is encrypted. If not, the packet (C) is passed directly to the decoder at 288 for decoding. If the packet is encrypted at 284, it is deemed to be an EA packet and is dropped or ignored at 278. In some implementations, the primary packet's encryption does not get checked at 284. Rather, its simple position relative to the secondary packet can be checked at 284 to identify it for replacement.

Please rewrite the paragraph starting on line 3 of page 24 to read:

Thus, each dual partially encrypted program has two sets of PIDs associated therewith. If, as described, the encryption is carried out on a period-by-period basis, for the system shown with an appropriate time slice interval, the picture will be essentially unviewable on a STB with either ~~neither~~ decryption.

Please rewrite the paragraph starting on line 17 of page 24 to read:

In systems where system A corresponds to legacy set-top boxes manufactured by Motorola or Scientific Atlanta, no modifications to the STBs are required. For the system B compliant STBs, for dual carriage of partially encrypted programs as described herein, the video and audio decoder are adapted to listen to two PIDs each (a primary and a secondary PID) instead of just one. There may be one or more secondary shadow PIDs, depending on the number of non-legacy CA systems in use, however a specific set-top box only listens to one of the secondary PIDs as appropriate for the CA method being used by that specific STB. In addition, ideally the encrypted packets from the PID carrying the mostly clear video or audio are ignored. Since ignoring "bad packets" (those that cannot be readily decoded as is) may already be a function that many decoders perform, thus requiring no modification. For systems with decoders that do not ignore bad packets, a filtering function can be used. It should be understood that the time slice encryption technique could be applied to just the video or the audio. Also, the video may be time slice encrypted while the audio is dual encrypted as in the earlier embodiment. The time slice technique may be applied to multiple programs concurrently. The number of programs that <u>are</u> encrypted during a period of time is mainly an issue of bandwidth allocation, and although the example discusses scrambling a single program at a time, the invention is not limited by that. Other combinations of encryption techniques described in this document will also occur to those skilled in the art.

Please rewrite the paragraph starting on line 5 of page 27 to read:

Those skilled in the art will recognize that many variations of the technique can be devised consistent with the partial scrambling concepts disclosed herein. For example, a pattern of five clear followed by two encrypted followed by two clear followed by one encrypted (CCCCCEECCECCCCCEECCE...) is consistent with variations of the present partial encryption concept, as are random, pseudo-random and semi-random values for M and N may be used for selection of packets to encrypt. Random, pseudo-random or semi-random (~~herein~~ collectively referred to as "random" herein) selection of packets can make it difficult for a hacker to algorithmically reconstruct packets in a post processing

attempt to recover recorded scrambled content. Those skilled in the art will understand how to adapt this information to the other embodiments of partial encryption described later herein. Some of the embodiments can be used in combination to more effectively secure the content.

Please rewrite the paragraph starting on line 15 of page 30 to read:

Referring now to **FIGURE 6,** a block diagram of a system consistent with an embodiment of the present invention in which portions of programming are dual encrypted on a packet-by-packet basis is illustrated as system 300. In this system, packets of each program are dual encrypted using, for example, legacy CA system A and new CA system B. The packets that are encrypted are selected based upon their importance to the proper decoding of the video and/or audio stream.

Please rewrite the paragraph starting on line 5 of page 31 to read:

MPEG (Moving Pictures Expert Group) compliant compressed video repackages the elementary data stream into the transport stream in somewhat arbitrary payloads of 188 bytes of data. As such, the transport stream packets containing a PES header can be selected for encryption at selector 316 and dual encrypted by both the CA system A encrypter 318 and the CA system B encrypter 324. Packets to be dual partially encrypted are duplicated and the PIDs of duplicate packets encrypted by encrypter 324 are remapped at 330 to a secondary PID as in the previous embodiment. The remaining packets are passed in the clear. The clear packets, system A encrypted packets, system B encrypted packets, ~~and~~ system information 328, and PSI from 329 are multiplexed together for broadcast over the cable system 32.

Please rewrite the paragraph starting on line 24 of page 31 to read:

Using video ~~is used~~ as an example, each sample is known as a frame and the sample rate is typically 30 frames per second. If the samples are encoded to fit into 3.8 Mbps, each frame would occupy 127K bits of bandwidth. This data is sliced for MPEG

transport into packets of 188 bytes with the first packet(s) of each frame containing the header used for instructions to process the body of the frame data. Dual encrypting just the first header packet (1504 additional bits) requires only 1.2% (1504/127K) of additional bandwidth. For high definition (19 Mbps) streams the percentage is even less.

Please rewrite the paragraph starting on line 3 of page 32 to read:

As previously stated, transport stream packets containing a PES header are the preferred target for encryption according to the present embodiment. These packets contain sequence headers, sequence extension headers, picture headers, quantization and other decode tables that also fall within the same packet. If these packets cannot be decoded (i.e., by a hacker attempting to view unauthorized programming without paying the subscription charges), not even small portions of the program can be viewed. In general, any attempt to tune to the program will likely be met with a blank screen and no audio whatsoever since known decoder integrated circuits use the PES header to sync up to an elementary stream such as video and audio in real-time. By encrypting the PES header, the decoding engine in an un-authorized set-top box cannot even get started. Post processing attacks, e.g. on stored content, are thwarted by ~~critical~~ dynamically changing information in the packet containing the PES header. Those skilled in the art will appreciate that for implementation of this embodiment of the invention, other critical or important packets or content elements may also be identified for encryption that could severely inhibit unauthorized viewing without departing from the present invention. For example, MPEG intra-coded or I frame picture packets could be encrypted to inhibit viewing of the video portion of the program. Embodiments consistent with the present invention may be used in any combination with other embodiments, e.g. scrambling the packet containing the PES header as well as random, M^{th} and N, or data structure encryption of the other packets. Critical packet encryption may be applied to video encryption, while a different method may be applied to audio. Audio could be dual encrypted, for instance. Other variations within the scope of the present invention will occur to those skilled in the art.

Please rewrite the paragraph starting on line 15 of page 34 to read:

Turning now to **FIGURE 9**, one embodiment of a system that minimizes the need for any additional bandwidth is illustrated as system 400. In this embodiment, the system takes advantage of the fact that system information (SI) 428 is required for a set-top box to tune programming. In a cable system, SI is sent ~~in the~~ out-of-band, at a frequency set aside from the normal viewing channels. It is possible to also ~~sent~~ send it in-band. If sent in-band, the SI 428 is replicated and sent with each stream. For discussion purposes, assume that the SI delivered to "legacy" set-top boxes from previous manufacturers is separate from the SI delivered to set-tops from new manufacturers such as STB 436. Consequently, each version of the SI can be independently scrambled as illustrated using conditional access system A 418 and conditional access system B 424. The clear video 404 and clear audio 406 are delivered in the clear, but in order to understand how to find them, the SI information 428 is needed.

Please rewrite the paragraph starting on line 5 of page 35 to read:

To frustrate a hacker who might program a set-top box to trial or scan frequencies, the frequencies for the channels can be offset from the standard frequencies. Also, the frequencies can be dynamically changed on a daily, weekly or other periodic or random basis. A typical cable headend may have roughly 30 frequencies in use. Each frequency is typically chosen to avoid interference between, among other things, each other, terrestrial broadcast signals, and frequencies used by clocks of the receiving equipment. Each channel has at least ~~1~~ one independent alternate frequency that if used would not ~~could not~~ cause interference, or cause the frequency of adjoining channels to be changed. The actual possible frequency maps are therefore 2^{30} or 1.07×10^9. However, a hacker might simply quickly try both frequencies on each tune attempt for each of the 30 channels or so. If successful in locating a frequency with content, the hacker's set-top box can then parse the PSI 429 to learn about the individual PIDs that make up a program. The hacker will have difficulty learning that "program 1" is "CNN", and that "program 5" is "TNN", and so on. That information is sent with the SI, which as stated above is

scrambled and otherwise unavailable to the un-authorized set-top box. However, a persistent hacker might yet figure those out by selecting each one and examining the content delivered. So in order to frustrate the identification of channels, the assignment of a program within a single stream can move around, e.g. program 2 and program 5 swapped in the example above so that "program 1" is "TNN" and "program 5" is "CNN". Also, it is possible to move programs to entirely different streams with entirely new program groupings. A typical digital cable headend can deliver 250 programs of content including music. Each can be uniquely tuned. The possible combinations for re-ordering are 250! (factorial). Without a map of the content provided by either the delivered SI or by a hacker, the user is faced with randomly selecting each program in a stream to see if it is the one interest.

Please rewrite the paragraph starting on line 3 of page 36 to read:

Thus, at headend 422, the video signal 404 and the audio signal 406 are provided in the clear (unencrypted) while the SI 428 is provided to multiple CA systems for delivery over the cable network. Thus, in the exemplary system 400, clear SI 428 is provided to an encryption system ~~428~~ 418 that encrypts SI data using encryption system A. Simultaneously, clear SI 428 is provided to encryption system 424 that encrypts the SI data using encryption system B. Clear video 404, ~~and~~ audio 406, and PSI 429 are then multiplexed along with encrypted SI from 418 (SI A) and encrypted ~~audio~~ SI from 424 (SI B) to replace out of band system information 428.

Please rewrite the paragraph starting on line 11 of page 36 to read:

After distribution through the cable system 32, the video, the audio, PSI, system information A and system information B are all delivered to set-top boxes 36 and 436. At STB 36, the encrypted SI is decrypted at CA system A 40 to provide tuning information to the set-top box. The set-top box tunes a particular program to allow it to be displayed on television set 44. Similarly, at STB 436, the encrypted SI is decrypted at CA system B 440

to provide tuning information for the set-top box, to allow a particular program to be tuned and displayed on television set 444.

Please rewrite the paragraph starting on line 6 of page 37 to read:

Each of the above techniques can be represented generically by the system 500 of **FIGURE 10**. This system 500 has a cable system headend 522 with clear video 504, clear audio 506, SI 528, and PSI 529 any of which can be selectively switched through an intelligent processor controlled switch 518, which also serves to assign PIDs (in embodiments requiring PID assignment or reassignment), to conditional access system A 520 ~~504~~ or conditional access system B 524 or passed in the clear to the cable system 32. As previously, the program or SI encrypted according to the legacy CA system A can be properly decoded by STB 36. The CA system B encrypted information is understood by STBs 536 and decrypted and decoded accordingly, as described previously.

Please rewrite the single-row table on line 9 of page 38 to read:

025C04	025E05	125E11	025C06	025C07	025C08	025C09	~~125E12~~ 025E10	125E12

Please rewrite the single-row table on line 20 of page 38 to read:

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

Please rewrite the single-row table on line 24 of page 38 to read:

125C04	025E11	125E05	125C06	125C07	125C08	125C09	~~125E10~~ 025E12	125E10

Please rewrite the paragraph starting on line 5 of page 39 to read:

The primary and secondary PIDs are conveyed to the STBs in the program map table (PMT) transmitted as a part of the program specific ~~system~~ information (PSI)

data stream. The existence of a secondary PID can be established to be ignored by the STB operating under CA encryption system A (the "legacy" system), but new STBs operating under CA encryption system B are programmed to recognize that secondary PIDs are used to convey the encrypted part of the program associated with the primary PID. The set-top boxes are alerted to the fact that this encryption scheme is being used by the presence of a CA descriptor in the elementary PID "for loop" of the PMT. There typically would be a CA descriptor for the video elementary PID "for loop", and another one in the audio elementary PID "for loop". The CA descriptor uses a Private Data Byte to identify the CA_PID as either the ECM PID or the secondary PID used for partial scrambling, thus setting up the STB operating under system B to look for both primary and secondary PIDs associated with a single program. Since the PID field in the transport header is thirteen bits in length, there are 2^{13} or 8,192 PIDs available for use, any spare PIDs can be utilized for the secondary PIDs as required.

Please rewrite the paragraph starting on line 1 of page 41 to read:

Packet selector / duplicator 610 selects packets that are to be dual encrypted under any of the above partial dual encryption methods. Those packets are then duplicated with new PIDs so that they can be later identified for encryption. For example, if packets at the input of 610 associated with a particular program have PID A, then packet selector / duplicator 610 identifies packets to be encrypted and duplicates those packets and remaps them to PIDs B and C respectively, so that they can be identified later for encryption under two different systems. Preferably, the duplicate packets are inserted into the data stream adjacent one another in the location of the originally duplicated packet now with PIDs B and C so that they remain in the same order originally presented (except that there are two packets where one previously resided in the data stream). Assume, for the moment, that the new CA system to be added is NDS encryption. In this case, PID A will represent clear packets, PID B will represent NDS encrypted packets and PID C will represent Motorola encrypted packets. The packets having PID B may be encrypted under the NDS encryption at this point in 610 or may be encrypted later.

Please rewrite the paragraph starting on line 17 of page 41 to read:

The packets with PIDs B and C are then returned to the system 604 where packets with PID C are encrypted under Motorola encryption at cable scrambler 612 as instructed by the control system 614 associated with the Motorola equipment. The output stream from cable scrambler 612 then proceeds to another new device - PID remapper and scrambler 620, which receives the output stream from 612 and now remaps the remaining packets with PID A to PID C and encrypts the PID B packets under the NDS encryption algorithm under control of control system 624. The output stream at 626 has clear unencrypted packets with PID C and selected packets which have been duplicated and encrypted under the Motorola encryption system with PID C along with encrypted packets under the NDS encryption system with PID B. This stream is then modulated (e.g., Quadrature Amplitude Modulated and RF modulated) at 628 for distribution over the cable system. The preferred embodiment maps the unencrypted packets on PID A to match the scrambled packets on PID C because the audio and video PIDs called out in legacy program specific information (PSI) ~~is~~ are correct that way. The control computer, the scrambler, and legacy set-top boxes only know about PID C. Alternatively, the scrambled packets on PID C could be mapped back to PID A, but this would likely mean editing the PSI, that was automatically generated, to map the PID numbers from PID C back to PID A in the PID remapper and scrambler 620.

Please rewrite the paragraph starting on line 27 of page 45 to read:

Selected PIDs can be stripped from the incoming transport via the STB's PID filter, decrypted and buffered in Synchronous Dynamic Random Access Memory (SDRAM), similar to the initial processing required in preparation for transfer to ~~an~~ a hard disk drive (HDD) in a Personal Video Recorder (PVR) application. The host CPU 916 can then "manually" filter the buffered data in SDRAM for elimination of the packets containing unneeded PIDs. There are some obvious side effects to this process.

Please rewrite the paragraph starting on line 18 of page 46 to read:

A second technique for implementation in a set-top box is illustrated in **FIGURE 15**. Since RISC processor A/V decoder module 934 in decoder circuit 930 processes the partial transport PIDs and strips/concatenates for decode, the firmware within decoder IC 930 can be altered to exclude individual packets in a partial transport stream based upon criteria in each packet header. Alternatively, the demultiplexer 910 can be designed to exclude the packets. Legacy scrambled packet(s) pass through the CA module still encrypted. By using the decoder IC 930 to perform the removal of the legacy scrambled packets and assuming that the packets encrypted under the new encryption algorithm (e.g., NDS) ~~is~~ are immediately adjacent the legacy encrypted packet (or at least prior to next primary stream video packet) then the pruning of the legacy packet in effect accomplishes the merging of a single, clear stream into the header strip and video queue.

Please rewrite the paragraph starting on line 1 of page 47 to read:

A third technique for implementation of partial decryption in a set-top box is illustrated in **FIGURE 16**. In this embodiment, the PID remapping is carried out either within a circuit such as an Application Specific Integrated Circuit (ASIC), Field Programmable Gate Array (FPGA), or a programmable logic device (PLD) 938 or other custom designed circuit placed between the tuner and demodulator 904 and the decoder IC 908. In a variation of this embodiment, the decoder IC 908 can be modified to implement the PID remapping within demultiplexer 940. In either case, the legacy encrypted packets are dropped and the non-legacy packets are re-mapped either in circuit 938 or demultiplexer 940.

Please rewrite the paragraph starting on line 10 of page 47 to read:

This third technique can be implemented in one embodiment using the PLD depicted in **FIGURE 17**. This implementation assumes that there will ~~be~~ not be more than one encrypted packet of a particular PID appearing in a row, thus, the implementation could be modified to accommodate bursts of encrypted packets such as with the M and N^{th} encryption arrangement described above (as will be explained later). The input stream

passes through a PID identifier 950 which serves to demultiplex the input stream based upon PID. Primary PID packets are checked for continuity at 958. If a continuity error is detected, the error is noted and the counter is reset at 960.